IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF WISCONSIN GREEN BAY DIVISION

JEANETTE ALONSO, on behalf of herself and all others similarly situated, Plaintiff, v. FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC Defendants.	Case No.: _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jeanette Alonso ("Plaintiff"), by and through the undersigned counsel, bring this Class Action Complaint against Defendants Forefront Dermatology, S.C. and Forefront Management, LLC (collectively, "Defendants," "Forefront Dermatology," or "Forefront"), on behalf of herself and all others similarly situated. Plaintiff make the following allegations based upon personal knowledge as to their own actions and upon information and belief as to all other matters.

INTRODUCTION

1. Forefront Dermatology is a Wisconsin-based dermatology practice group that holds itself out as "one of the nation's largest physician led and operated dermatology group practices." Between May 28 and June 4, 2021, hackers gained access to Forefront's information technology (IT) systems and encrypted troves of highly sensitive files, demanding a ransom in exchange for the decryption keys (the "Data Breach").

2. The information accessed included Forefront employees' full names, home addresses, and social security numbers, and Forefront patients' full names, home addresses, dates

of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information (collectively, "PII"). After Forefront failed to meet the hackers' demands, the data was exfiltrated and portions were posted to a dark web website associated with a well-known ransomware group known as "Cuba Ransomware," where it is available for anyone to download.

3. Despite notifying more than 2.4 million people that their PII was exposed, Forefront has attempted to downplay the severity of the breach by withholding key details surrounding the Data Breach, including the nature of the attack, the identity of the hackers, and the fact that stolen data is available for download and purchase on underground websites.

4. Forefront Dermatology failed to secure its databases containing massive amounts of PII, failed to detect the hackers' presence, and failed to take any steps to investigate the numerous other red flags that should have warned the company that its systems were not secure.

5. As a result of Forefront Dermatology's failure to protect the information it was entrusted to safeguard, Plaintiff and class members did not receive the benefit of their bargain with Forefront and now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

6. Plaintiff Jeanette Alonso is a patient of Forefront Dermatology and current resident and citizen of Orland Park, Illinois.

7. Defendant Forefront Dermatology, S.C. is a Wisconsin services corporation with its principal place of business located at 801 York Street, Manitowoc, Wisconsin 54220.

8. Defendant Forefront Management, LLC is a Delaware company registered to do business in Wisconsin and with its principal place of business located at 801 York Street, Manitowoc, Wisconsin 54220.

9. Both Defendants, Forefront Dermatology, S.C. and Forefront Management, LLC, have jointly stated that the data breach described herein occurred to their systems.[1]

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000.00 exclusive of interest and costs, there are more than 100 putative Class Members, and minimal diversity exists because Plaintiff and many putative class members are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

11. This Court has personal jurisdiction over the Defendants because they are headquartered in and/or maintain their principal places of business in this District. Defendants are authorized to and regularly conduct business in this District and make decisions regarding corporate governance and management, including decisions regarding the security measures to protect its patients' and employees' PII within this District. Defendants intentionally avail themselves of this jurisdiction by promoting, selling, and marketing their services from Wisconsin to individuals across the country.

12. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendants' headquarters and principal place of business are located in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel that led to the Data Breach.

[1] *See, e.g.,* https://www.hipaanswers.com/data-breach-affecting-2-41-million-individuals-reported-by-wisconsin-dermatology-practice/ (last visited September 21, 2021); https://www.hipaajournal.com/wisconsin-dermatology-practice-reports-data-breach-affecting-4400-individuals/ (last visited September 21, 2021)

FACTUAL ALLEGATIONS

Forefront Dermatology's Business Model and Data Collection Practices

13. Forefront Dermatology is a Wisconsin-based dermatology practice group that partners with nearly 200 board-certified dermatologists practicing in over 180 locations across 21 states. Forefront Dermatology states that its "goal is to make it easier for you to find the board-certified, expert dermatology care you need within your own community—and without waiting weeks to be seen."[2]

14. Forefront Dermatology entices dermatologists to partner with its practice by offering "shared support services"[3] that include the following shared functions:

- Accounting
- Billing and collections
- Business development
- Compliance
- Credentialing
- Dermatopathology Lab
- Human Resources
- IT Resources
- Legal
- Marketing
- Payroll
- Scheduling Concierge

15. By taking over all administrative functions associated with operating a medical practice, Forefront promotes the partnership as a means to "remove the burden of your administrative duties so you can enjoy more stress-free time outside of the office. All physicians

[2] https://forefrontdermatology.com/about-us/ (last visited August 10, 2021).

[3] https://joindermsuccess.com/the-forefront-difference/ (last visited August 10, 2021).

are given full autonomy to run their own practice while benefiting from the support of [Forefront's] centralized services." [4]

16. Forefront's business has been wildly successful. In 2016, Forefront Dermatology was acquired by Toronto, Canada-based OMERS Private Equity group at a time when it operated around 82 clinics in 11 states and generated $30 million in annual earnings before interest, taxes, depreciation, and amortization (EBITDA).[5] Over the last five years, Forefront has expanded its platform to more than 195 board-certified dermatologists across 21 states and is projecting around $100 million in adjusted 2021 EBITDA. Recent reports suggest that OMERS is preparing to sell the company at a valuation of $1.6 to $1.8 billion.[6]

17. Of course, a business model dependent on rapid expansion and the centralization of services such as employee payroll, patient scheduling, billing, and lab results, requires significant investment in information technology and data security given the massive amounts of highly sensitive information Forefront must collect, store, and manage.

18. For example, for partner dermatologists to utilize Forefront's centralized payroll features, Forefront must collect and store, among other sensitive information, employees' full names, addresses, dates of birth, Social Security numbers, banking information, payroll tax forms, and health insurance information for themselves and their dependents.

19. Likewise, in the course of providing medical services, Forefront requires patients to provide personal information including their full names, home addresses, dates of birth, email addresses, and Social Security numbers, financial information such as bank account and payment

[4] *Id*.

[5] https://www.pehub.com/next-up-in-physician-practice-management-omers-readies-sale-of-forefront-dermatology/ (subscription required) (last visited August 10, 2021).

[6] *Id*.

card numbers, and medical information including medical histories, past treatment records, prescription information, health provider information, and health insurance coverage. As a result, when patients are treated by a Forefront-affiliated practice group, their highly sensitive PII is stored on centralized servers maintained by Forefront.

20. Given the amount and sensitive nature of the data it collects, Forefront maintains a "Privacy Policy"[7] effective July 10, 2019, relating to the use of its website and a "Notice of Privacy Practices"[8] effective April 23, 2021, that "describes how medical information about you may be used and disclosed" in the course of providing health care services.

21. Relating to use of its website, the Privacy Policy provides in pertinent part that:

> **Information Collected**
> Forefront Dermatology collects several types of information via the Website:
>
> **Personal Information**: Forefront Dermatology may collect personal information that identifies you as an individual ("Personal Information") such as name, e-mail address, mailing address, phone number, age and or date of birth, gender, insurance information, health and medical information or other protected health information, account numbers, financial and payment information such as credit card information, and any other information you choose to provide us.[9]

22. Forefront's "Notice of Privacy Practices" states that "[i]t is your right as a patient to be informed of Forefront Dermatology's legal duties with respect to protection of the privacy of your protected health information ("PHI")."[10] Among other representations, Forefront promises that it "will not use or disclose your PHI without your authorization" and that "disclosures of PHI not described in this Notice will be made only with your authorization."[11]

---

[7] https://forefrontdermatology.com/privacy-policy/ (last visited August 10, 2021).

[8] https://forefrontdermatology.com/wp-content/uploads/2021/05/Forefront-Dermatology-Affiliated-Practices-NOPP-1.pdf (last visited August 10, 2021).

[9] https://forefrontdermatology.com/privacy-policy/ (last visited August 10, 2021).

[10] https://forefrontdermatology.com/wp-content/uploads/2021/05/Forefront-Dermatology-Affiliated-Practices-NOPP-1.pdf (last visited August 10, 2021).

[11] *Id*.

The Data Breach and Cuba Ransomware

23. On July 8, 2021, Forefront Dermatology posted a notice on its website entitled "Notice of Data Security Incident."[12] The notice stated that "[o]n June 24, 2021, Forefront Dermatology, S.C. and its affiliated practices concluded its investigation of an intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain patient information. The company first identified the intrusion on June 4, 2021, and immediately took its network offline to protect the information it maintains and secure its systems. In addition, it promptly launched an investigation and notified law enforcement."[13]

24. The notice further provided that "[t]he investigation determined that unauthorized parties gained access to Forefront Dermatology's IT network between the dates of May 28, 2021 and June 4, 2021 and accessed certain files that contain information pertaining to some patients. This information may have included patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information."[14]

25. After discovery of the Data Breach, Forefront stated that it "immediately took its entire network offline out of an abundance of caution to protect its patients and to secure its systems. Forefront also launched an investigation and notified law enforcement. Once Forefront determined that personal information was potentially involved in this incident, it moved quickly

[12] https://forefrontdermatology.com/incidentnotice/ (last visited August 10, 2021).

[13] *Id.*

[14] *Id.*

to notify those individuals and government regulators, in accordance with applicable law. To help prevent something like this from happening again, Forefront Dermatology is enhancing its security protocols."[15]

26. Forefront advised victims "to review the statements they receive from their health care providers and health insurance plan. If individuals see services they did not receive, they should contact the provider or health plan immediately."[16]

27. Forefront later reported to the U.S. Department of Health and Human Services Office for Civil Rights, which requires notice of breaches involving protected health information ("PHI"), that 2,413,553 individuals had their PHI compromised in the Data Breach—resulting in the third largest breach involving PHI in the United States over the last two years.[17]

28. Both Defendants, Forefront Dermatology, S.C. and Forefront Management, LLC, jointly reported to various state authorities that their systems had been breached.[18]

29. On July 9, 2021, the website databreaches.net posted an article revealing key details surrounding the Data Breach that were not included in Forefront's notice.[19] In particular, the article revealed that the nature of the attack was a "ransomware" attack whereby hackers gained unauthorized access to Forefront's systems and deployed a form of malware designed to encrypt the files in the database rendering them unusable. The hackers then demand a ransom in exchange

[15] *Id*.

[16] *Id*.

[17] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited August 10, 2021).

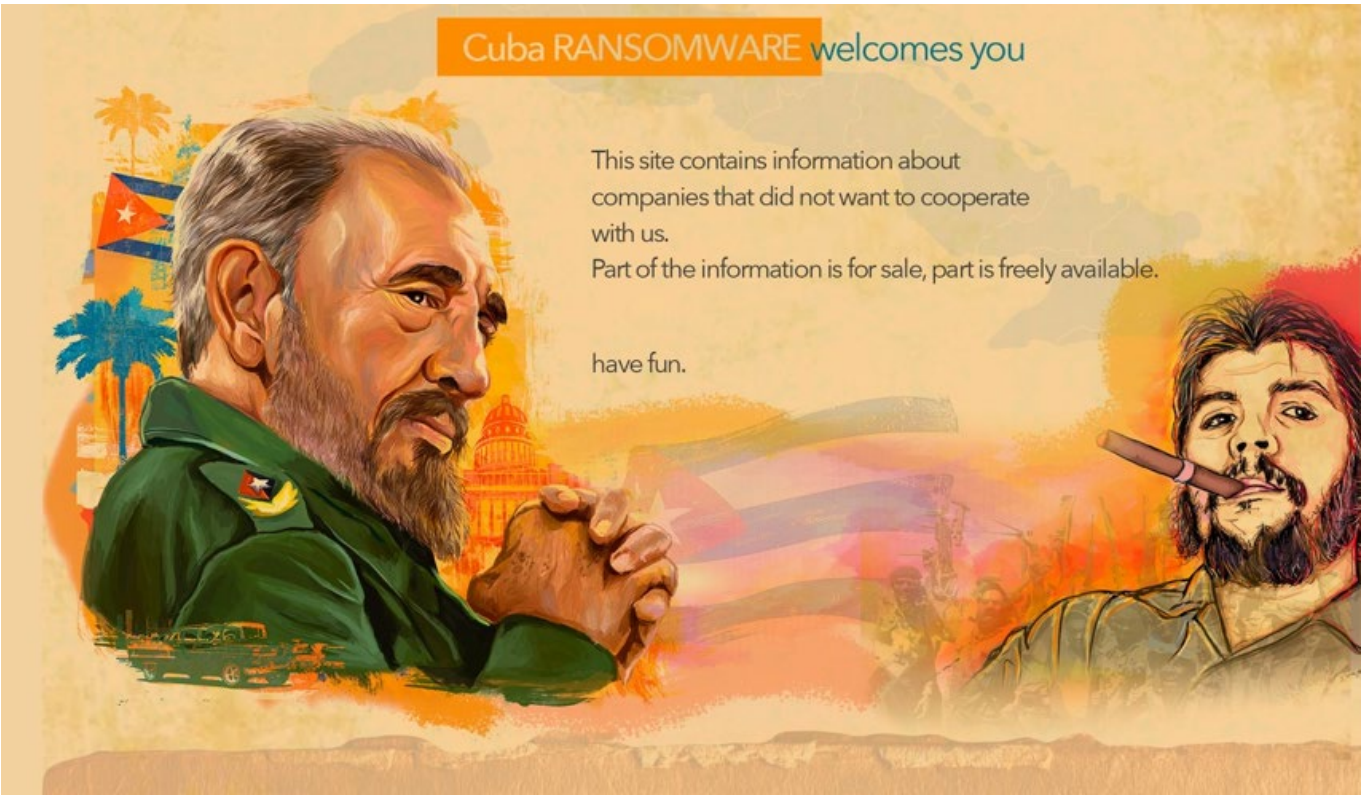
[18] *See, e.g,* https://apps.web.maine.gov/online/aeviewer/ME/40/f3f9c506-728b-4271-9497-95ce115e2fd0.shtml (last visited September 21, 2021); https://oag.ca.gov/ecrime/databreach/reports/sb24-542688 (last visited September 21, 2021); https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM10808.pdf (last visited September 21, 2021).

[19] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (last visited August 10, 2021).

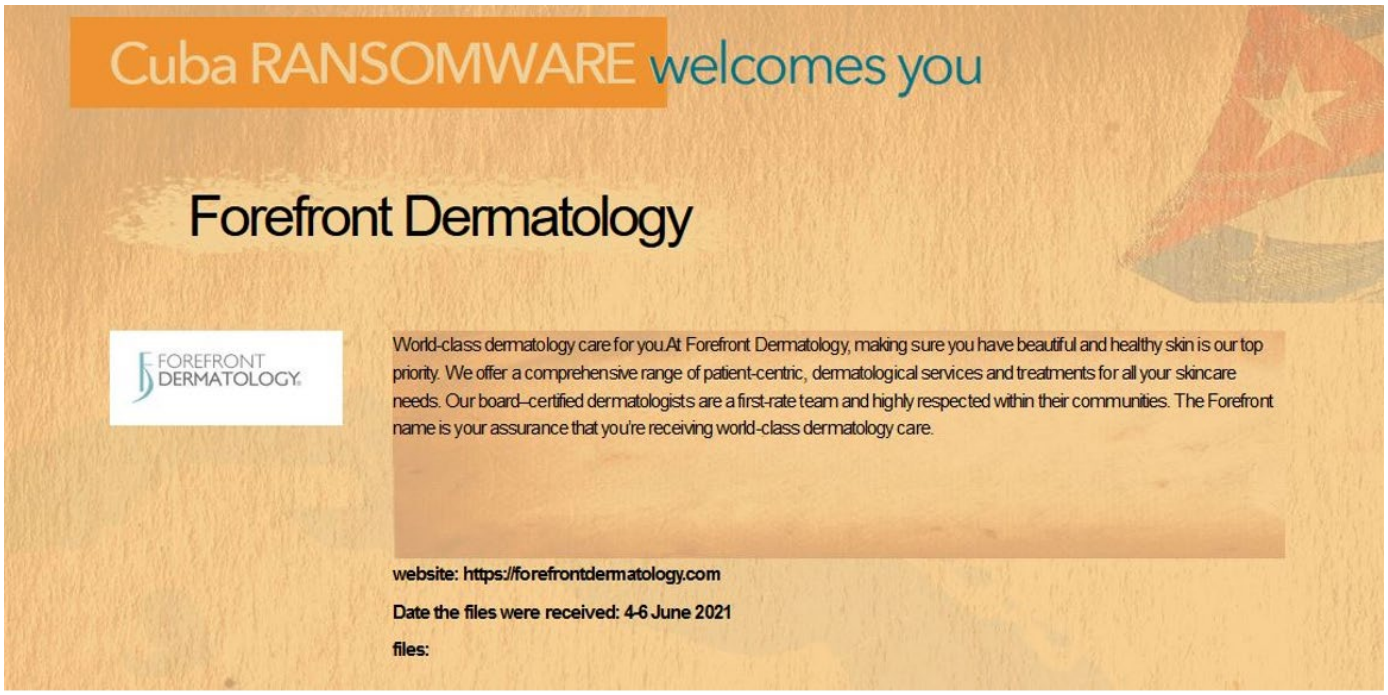
for the decryption keys. If their demands are not met, the hackers will exfiltrate the information and seek to profit from it in other ways including selling it on underground markets.

30. And that is precisely what happened here. The databreaches.net article noted that in June 2021 a ransomware group known as Cuba Ransomware ("Cuba") released portions of the stolen data on its underground website accessible on the "dark web." The dark web is a portion of the Internet that is intentionally hidden from search engines and requires the use of an anonymizing browser to be accessed. It is most widely used as an underground black market where individuals sell illegal products like drugs, weapons, counterfeit money, and sensitive stolen data that can be used to commit identity theft or fraud.

31. Cuba's dark web website is welcoming to fraudsters and thieves, advertising that "[t]his site contains information about companies that did not want to cooperate with us. Part of the information is for sale, part is freely available. have fun." A screenshot is provided below:



32. The website contains separate pages hosting information from breaches Cuba claims credit for, including a webpage dedicated specifically to the Forefront breach. The webpage provides a description of Forefront, the company's logo, website URL, and a note that the files were received between June 4-6, 2021.



33. Consistent with its regular practice, Cuba elected to release portions of the data free of charge so fraudsters could sample it and confirm that Cuba had the data in its possession. The rest it will sell to any fraudster who is willing to pay for it. The databreaches.net article reported that the June 2021 sample data dump included 47 megabytes of data containing "some patient information" and "more than 130 files with information on the entity's system and network, with security and backup details, and all their logins to health insurance portals, etc." [20]

34. The sample data dump also included credentials including usernames, passwords, and security questions utilized by Forefront patients to access their insurer's login portals.

[20] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (last visited August 10, 2021).

User	User Name	Password	Security Questions	Email address
REDACTED	REDACTED	dawderm3	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	REDACTED
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		600York	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		forefront4!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Forefront1!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	

35. Although not disclosed by Forefront, cybersecurity research firms have authored investigative reports analyzing Cuba's methods in conducting ransomware attacks. In a joint report entitled *Cuba Ransomware Group on a Roll*, cybersecurity firms Proferro and Security Joes issued a joint report addressing Cuba's *modus operandi* and ransomware tactics in other large-scale breaches.[21] Several conclusions from the report are relevant here.

36. First, Cuba is comprised of Russian speakers who "are not state-sponsored, instead operating simply as a threat group. They are fast acting, and seem to prefer to communicate via email—they generally launch their attacks by setting up email accounts to initiate communication a few days in advance of deploying ransomware."[22] This brings Cuba's motive into focus: it wants to profit from the ransom or sale of a company's data.

37. Second, the group is sophisticated. The report notes that after Cuba gains access to a company's internal systems, "Cuba begins to encrypt all files on the infected machine, dropping its ransom note to each directory under the name '**!!FAQ for Decryption!!.txt**.' Unlike other ransomware families, the ransom note does not include a key for identification—it is more

[21] https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-+on+a+roll.pdf (last visited August 10, 2021).

[22] *Id*. at 2.

sophisticated, indicating this threat group likely performs a low volume of attacks against high-value organizations. The Cuba note informs the victim that all their files are encrypted, and invites them to contact the group via email to send payment in exchange for a decryptor."[23]

38. Third, Cuba uses the "RSA" encryption method as the means of conducting ransomware attacks. Under this method, files are encrypted with a code called a public key, which can be shared openly, and, once encrypted, can only be decrypted with a separate private key provided by the hacker. The report notes that this method "allows operators behind Cuba ransomware to generate completely random encryption keys for each file—and to still be able to decrypt them even after payment has been received."[24] Thus, Cuba can prove it is able to decrypt information by providing a private key that will work to decrypt one file and then demand a ransom (usually in bitcoin) to decrypt the remaining files.

39. The report concludes that "[w]hile the Cuba Ransomware group has been around for some time, it only established itself as a major player recently, when the attackers breached the Automatic Funds Transfer Service and hosted stolen files on their Tor [dark web] site, which they then made accessible to others, for a fee. Prior to that, they targeted several companies in wide-ranging sectors, including a logistics company, a real estate firm, and an aviation company." [25] The report notes that there is no known motive for Cuba beyond a financial one in determining which companies to target.

40. Despite the obvious severity of the Data Breach, Forefront Dermatology was content to keep victims completely in the dark about what actually occurred. Nowhere in the notice

[23] *Id*. at 3.

[24] *Id*. at 7.

[25] *Id*. at 14.

posted on its website or in the individual data breach notification letters it sent to affected individuals did Forefront disclose the nature of the attack, the identity of the hackers, or the fact that the data had already been released and offered for sale on Cuba's website. Forefront's decision to downplay the severity of the Data Breach by withholding these key details has likely prevented millions of victims from appreciating the severity of the breach and taking measures that could help prevent or mitigate against identity theft or fraud.

The Data Breach was Preventable

41. Following the Data Breach, Forefront repeatedly stated that it was "enhancing its security protocols" in order to "prevent something like this from happening again."[26] But the "enhancements" undertaken by Forefront are industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks and that ransomware attacks have increased precipitously over the last several years.

42. Healthcare providers like Forefront Dermatology are prime targets because of the information they collect and store, including financial information of patients, online login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

43. This was known and obvious to Forefront Dermatology as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers. As reflected in the below chart, many of the largest breaches over the last decade have involved the theft of patient records from healthcare providers:

[26] https://forefrontdermatology.com/incidentnotice/ (last visited August 10, 2021).

Largest Healthcare Data Breaches (2009-2020)

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
4	Excellus Health Plan, Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
5	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss
6	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
7	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident

44. According to a report by the HIPAA Journal, "data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years, with 2020 seeing more data breaches reported than any other year since records first started being published."[27] In fact, healthcare data breaches were up 55% in 2020 from the prior year alone.[28]

45. Ransomware attacks in particular have been on the rise. According to cybersecurity firm SonicWall's 2021 Cyber Threat Report, ransomware attacks rose by 62% worldwide between

[27] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited August 10, 2021).

[28] https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/ (last visited August 10, 2021).

2019 and 2020, and by 158% in North America alone.[29] Verizon's 2021 Data Breach Investigations Report similarly notes that "[t]his year, we're displeased to report that we've seen yet another increase in Ransomware cases, which has been continuing on an upward trend since 2016 … The novel fact is that 10% of all breaches now involve Ransomware. This is because [threat actors] have adopted the new tactic of stealing the data and publishing it instead of just encrypting it."[30]

46. The risk is so prevalent for healthcare providers that on October 28, 2020, the Federal Bureau of Investigation (FBI) and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[31] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[32]

47. Specifically, the joint advisory encouraged healthcare providers to follow the guidance set forth in the CISA's September 2020 Ransomware Guide ("CISA Ransomware Guide"), which sets forth detailed ransomware prevention best practices and response strategy.[33]

---

[29] https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/ (last visited August 10, 2021).

[30] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited August 10, 2021).

[31] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited August 10, 2021).

[32] *Id*.

[33] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited August 10, 2021).

48. Although Forefront did not disclose how Cuba was able to gain unauthorized access to its systems in the first instance, history shows that the use of stolen credentials through "phishing" scams have long been the most popular and effective method of gaining authorized access to a company's internal networks.

49. There are two primary defenses to "phishing" scams: employee education and technical security barriers. Employee education is the process of making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

50. Employee education provides the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of sensitive internal information. The CISA Ransomware Guide notes that companies housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[34]

51. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions,

[34] CISA Ransomware Guide at 5.

including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[35]

52. Additionally, because the goal of many phishing attempts is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if a phishing attempt is successful. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

53. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information

[35] *Id.*

or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

54. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[36] In an example given by security software provider Digital Guardian, "an employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide."[37] This is why approximately 67% of targeted malware and phishing attacks are directed at individual contributors and lower-level management personnel.[38]

55. In addition to addressing "phishing" attempts, the CISA Ransomware Guide encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

[36] https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited August 10, 2021).

[37] *Id*.

[38] https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited August 10, 2020).

- Ensuring devices are properly configured and that security features are enabled;
- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[39]

56. The CISA Ransomware Guide further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[40]

57. Despite holding the PII of millions of individuals nationwide and electing to store that information in a centralized location, Forefront Dermatology failed to adhere to these recommended best practices. In addition to lacking the necessary safeguards to secure PII, Forefront Dermatology did not have adequate network segmentation or monitoring systems in place to detect the unauthorized infiltration after it occurred, which permitted Cuba to gain unauthorized to access Forefront's systems, move laterally undetected for days, locate and target the most sensitive data, and encrypt and exfiltrate that data for purposes of profiting from it. Forefront, like any healthcare provider its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient and employee files.

[39] CISA Ransomware Guide at 4.

[40] *Id*. at 5.

58. Forefront had the knowledge and resources to prevent a breach—and in fact made significant expenditures to promote its rapidly-growing dermatology practice—but neglected to make corresponding investments in data security to ensure the millions of sensitive files in its possession were securely stored. Forefront's implementation of "enhanced" security measures only after the fact is inexcusable given its knowledge that it was a prime target for cyberattacks.

Allegations Relating to Plaintiff Jeanette Alonso

59. Plaintiff Jeanette Alonso lives and resides in Orland Park, Illinois.

60. Plaintiff first received medical care in August, 2020 from Forefront Dermatology located in Berwyn, Illinois.

61. Before Forefront Dermatology would see Plaintiff as a patient, she was required to provide Forefront with her sensitive personal information, including, among other information, her full name, home address, dates of birth, e-mail addresses, social security numbers, health insurance ID cards, driver's license and medical history.

62. Forefront also maintained Plaintiff's patient account number, health insurance plan member ID number, medical record number, dates of service, provider names, and medical and clinical treatment information.

63. In or about July 2021, Plaintiff received a notification letter from Forefront Dermatology informing her that she was a victim of a data breach. The letter stated that, "**While our investigation did not find evidence that your information was specifically involved**, we could not rule out the possibility that files containing some of our patient information may have been subject to unauthorized access as a result of this incident. This information may have included some of your information that Forefront Dermatology has on file, including name in combination with your address, date of birth, patient account number, health insurance plan member ID number,

medical record number, dates of service, provider names, and/or medical and clinical treatment information."

64. The letter recommended that Plaintiff "review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately."

65. Forefront's letter created more questions than it answered. First, Forefront did not explain its irresolute statement that it "did not find evidence" the Plaintiff's PII was "specifically involved" yet could not rule out that it "may have been subject to unauthorized access." Presumably the database that Cuba gained unauthorized access to contained the sensitive information of Forefront's employees and patients. Cuba then encrypted and exfiltrated that data after its ransom demands were not met. Under these facts, it is inconceivable that Plaintiff's information would not have been included in the breach and Forefront's attempt to downplay that fact for supposed lack of evidence is misleading and deceptive.

66. Second, the letters did not explain the nature of the attack, the identity of the hackers, the number of individuals affected, or the fact that the information had already been released and listed for sale on the dark web. Forefront's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By failing to provide these material facts, Forefront prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from years of harm.

67. Finally, the letters provided no means of recourse for victims. Forefront did not provide meaningful guidance on how victims can protect themselves, offer compensation for losses caused by the breach, or even offer credit monitoring services to allow for victims to better

monitor their accounts for unauthorized activity. All Forefront provided was a phone number connecting victims to a call center representative who could provide scripted responses with no additional information beyond what was already contained in the letter.

68. Due to Forefront's woefully deficient notification, Plaintiff spent time conducting her own research into the breach, and spent time and effort signing up for services to monitor her credit, as well as reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do for years into the future. Plaintiff also suffered emotional distress knowing that her medical information is now available for sale and can be used to commit blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

Forefront Failed to Comply with Federal Law and Regulatory Guidance

69. Forefront Dermatology is a healthcare provider covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

71. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[41]

72. HIPAA requires that Forefront Dermatology implement appropriate safeguards for this information.[42]

73. HIPAA requires that Forefront Dermatology provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.[43]

74. Despite these requirements, Forefront Dermatology failed to comply with its duties under HIPAA and its own Notice of Privacy Practices. Indeed, Forefront failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PII of its patients and employees;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding

[41] 45 C.F.R. § 164.502.

[42] 45 C.F.R. § 164.530(c)(1).

[43] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

75. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[44]

76. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[45] Among other things, the guidelines note that businesses should protect the personal customer information that they collect and store; properly dispose of personal information that is no longer needed; encrypt information stored on their computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[46]

---

[44] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited August 10, 2021).

[45] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 10, 2021).

[46] *Id*.

77. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[47] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA Ransomware Guide.

78. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[48]

79. Here, Forefront Dermatology was fully aware of its obligation to implement and use reasonable measures to protect the PII of its employees and patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Forefront Dermatology's failure to employ reasonable measures to protect against unauthorized access to patient and employee information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

80. Given the highly sensitive nature of the PII stolen in the Data Breach, and its subsequent publication on the dark web, fraudsters across the globe now have the ability to commit

[47] FTC, *Start With Security*, *supra* note 41.

[48] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited August 10, 2021).

medical identity theft, financial fraud, and other identity-related fraud against Plaintiff and class members now and indefinitely into the future.

81. The PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

82. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[49]

83. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[50] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[51]

84. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies, "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical

[49] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited August 10, 2021).

[50] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited August 10, 2021).

[51] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited August 10, 2021).

records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[52]

85. Indeed, while federal law generally limits individuals' liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[53] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[54]

86. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an

[52] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited August 10, 2021).

[53] https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study") (last visited August 10, 2021).

[54] *Id*. at 9.

imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[55]

87. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[56]

88. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[57] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[58]

89. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;

[55] *Id*. at 2.

[56] *Id*. at 14.

[57] *Id*. at 1.

[58] *Id*.

- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[59]

90. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft." [60] This echoes the Ponemon study, which notes that "many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[61]

91. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives." [62] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[63]

---

[59] https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited August 10, 2021).

[60] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited August 10, 2021).

[61] Ponemon Study at 1.

[62] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited August 10, 2021).

[63] *Id.*

92. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[64] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[65] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

93. Given how quickly Cuba released the stolen data, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiff and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing healthcare and financial statements, checking credit reports, and spending time and effort searching for unauthorized activity.

94. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members

[64] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited August 10, 2021).

[65] *Id.*

- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.[66]

95. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[67]

96. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

97. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed

[66] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited August 10, 2021).

[67] *Id.*

by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

98. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their PII;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

99. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

100. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[68]

101. Plaintiff and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[69]

102. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had Forefront's patients known the truth about Forefront Dermatology's data security practices—that it did not adequately protect and store their PII —they would not have sought medical care from Forefront or would have paid

[68] http://www.gao.gov/new.items/d07737.pdf (last visited August 10, 2021).

[69] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited August 10, 2021).

significantly less. As such, Plaintiff and class members did not receive the benefit of their bargain with Defendants because they paid for the value of services they did not receive.

103. Plaintiff have a direct interest in Forefront Dermatology's promises and duties to protect their PII, *i.e.*, that Forefront *not increase* their risk of identity theft and fraud. Because Forefront failed to live up to its promises and duties in this respect, Plaintiff and class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Forefront Dermatology's wrongful conduct. Through this remedy, Plaintiff and class members seek to restore themselves and class members as close to the same position as they would have occupied but for Forefront Dermatology's wrongful conduct, namely its failure to adequately protect Plaintiff's PII.

104. Plaintiff further seek to recover the value of the unauthorized access to their PII permitted through Forefront's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and class members have a protectible property interest in their PII; (b) the minimum damages measure for the

unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

105. Forefront Dermatology continues to hold the PII of Plaintiff and class members, and, therefore, Plaintiff have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

106. Plaintiff seeks relief on behalf of herself and as representatives of all other persons who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

> All individuals whose PII was compromised as a result of the data breach announced by Forefront Dermatology on or about July 8, 2021 (the "Class").

107. Pursuant to Rule 23, Plaintiff asserts claims on behalf of a separate patient subclass defined as follows:

> All patients of Forefront Dermatology whose PII was compromised as a result of the data breach announced by Forefront Dermatology on or about July 8, 2021 (the "Patient Class").

108. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Class, Plaintiff asserts claims on behalf of a separate statewide subclass defined as follows:

> All individuals residing in Illinois whose PII was compromised as a result of the data breach announced by Forefront Dermatology on or about July 8, 2021 (the "Illinois Subclass").

109. Excluded from the Class and Subclass are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

110. Plaintiff reserves the right to propose other subclasses and amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

111. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical as there are potentially 2.4 million or more individuals whose PII was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. mail, internet postings, and/or published notice.

112. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include, but are not limited to:

a. Whether Forefront Dermatology knew or should have known of the susceptibility of its systems to a data breach;

b. Whether Forefront Dermatology failed to implement reasonable and adequate security procedures and practices;

c. Whether Forefront Dermatology's security measures to protect its systems were reasonable in light of known legal requirements;

d. Whether Forefront Dermatology took adequate measures to protect Plaintiff and class members' PII after evidence of unauthorized access on its network was discovered;

e. Whether Forefront Dermatology owed a duty to Plaintiff and class members to protect their PII;

f. Whether Forefront Dermatology breached its duty to protect the PII of Plaintiff and class members by failing to provide adequate data security;

g. Whether Forefront Dermatology's conduct, including its failure to act, resulted in or was the proximate cause of the breach and/or the loss of the PII of Plaintiff and

class members;

h. Whether Forefront Dermatology had a contractual obligation to use reasonable security measures and whether they complied with such contractual obligations;

i. Whether, as a result of Forefront Dermatology's conduct, Plaintiff and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

j. Whether, as a result of Forefront Dermatology's conduct, Plaintiff and class members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

113. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other class members. Like other class members, Plaintiff's PII was in Forefront Dermatology's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other class members and Plaintiff seeks relief consistent with the relief of the Class.

114. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate class representative because her interests do not conflict with the interests of class members she seeks to represent. Plaintiff retained counsel that is competent and experienced in complex class actions and data breach and privacy litigation. Plaintiff and her counsel intend to vigorously prosecute this action and to fairly and adequately protect the interests of class members.

115. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual

litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

116. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

117. Likewise, particular issues are appropriate for certification under Rule 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to, whether Forefront Dermatology owed a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their PII and whether Forefront Dermatology failed to take reasonable steps to safeguard the PII of Plaintiff and class members.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

118. Plaintiff restates and re-allege the preceding paragraphs as if fully set forth herein.

119. Defendants required Plaintiff and class members to submit PII as a condition of employment or receiving treatment at Forefront Dermatology. Defendants collected and stored the data for purposes of employment and treatment as well as for commercial gain.

120. Defendants had a non-delegable duty to ensure that the information they collected and stored and that any associated entities with whom they shared employee and patient information maintained adequate and commercially reasonable data security practices to ensure the protection of members' PII.

121. Defendants owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting the PII within their control from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Indeed, Defendants acknowledged this duty in Forefront's Notice of Privacy Policy, in which Forefront promised to protect Plaintiff's and class members' PII.

122. Defendants owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that Forefront Dermatology's systems and networks adequately protected the PII.

123. Defendants' duty to use reasonable care in protecting PII arose as a result of the common law and federal law, including the HIPAA regulations described above, as well as Defendants' own policies and promises regarding privacy and data security.

124. Defendants knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, the vulnerabilities in Forefront Dermatology's systems, and the importance of adequate security.

125. Defendants breached their common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients' PII and by omitting material information from the Data Breach notice provided to class members.

126. Defendants breached their duties to Plaintiff and class members in numerous ways, as described herein, including by:

a. failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and class members;

b. failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

c. failing to comply with their own privacy policies;

d. failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. failing to adequately monitor, evaluate, and ensure the security of Forefront Dermatology's network and systems;

f. failing to recognize in a timely manner that the PII of Plaintiff and Class Members had been compromised;

g. failing to disclose timely and adequately that the PII of Plaintiff and Class Members had been compromised.

127. Plaintiff's and class members' PII would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

128. Defendants' failure to take proper security measures to protect sensitive PII of Plaintiff and class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII. Given that healthcare providers are prime targets for hackers, Plaintiff and class members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Forefront Dermatology.

129. It was also foreseeable that Defendants' failure to provide complete and forthright notice of the Data Breach would result in injury to Plaintiff and class members.

130. As a direct and proximate result of Defendants' conduct, Plaintiff and class members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented publication of their PII; (iii) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Forefront Dermatology fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

131. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

132. As a healthcare provider, Defendants are entities covered by HIPAA, 45 C.F.R. § 160.102, and are therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

133. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

134. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation

specifications adopted under this part" apply to covered entities and their business associates, such as Forefront Dermatology.

135. Defendants are obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

136. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

137. Defendants violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

138. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id.*

139. Defendants breached their notification obligations under HIPAA by failing to give

complete and forthright notice of the breach to Plaintiff and class members.

140. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

141. HIPAA further requires Defendants to disclose the unauthorized access and theft of the PII to Plaintiff and the Class "without unreasonable delay" so that Plaintiff and class members can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PII. *See* 45 C.F.R. § 164.404.

142. Defendants violated HIPAA by failing to reasonably protect Plaintiff's and class members' PII and by failing to give complete and forthright notice, as described herein.

143. Defendants' violations of HIPAA constitute negligence *per se*.

144. Plaintiff and class members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

145. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

146. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

147. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

148. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and class members.

149. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

150. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

151. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and class members.

152. As a direct and proximate result of Defendants' negligence *per se* under HIPAA and the FTC Act, Plaintiff and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Patient Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

153. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

154. Forefront Dermatology disseminated a "Notice of Privacy Practices" ("Notice") to its patients which constitutes an agreement between Defendants and persons who provided their PII to Defendants, including Plaintiff and class members.

155. Plaintiff and class members formed a contract with Forefront Dermatology and

complied with all obligations under such contract when they provided PII to Defendants subject to the Notice.

156. Forefront's Notice states that it "will not use or disclose your PHI without your authorization" and that "disclosures of PHI not described in this Notice will be made only with your authorization." The nature of Defendants' express promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and class members' PII in order to prevent harm and prevent present and continuing increased risk.

157. Defendants breached their agreements with Plaintiff and class members when Forefront Dermatology disclosed Plaintiff's and class members' PHI without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notice.

158. As a direct and proximate result of these breaches, Plaintiff and class members sustained actual losses and damages as described in detail above, including that they did not receive the benefits of the bargains for which they paid, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

159. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein and assert this claim in the alternative to their breach of contract claims to the extent necessary.

160. Plaintiff and class members were required to provide their PII to Forefront Dermatology in order to receive healthcare services and treatment and/or for purposes of employment.

161. As part of these transactions, Defendants agreed to safeguard and protect the PII of Plaintiff and class members. Implicit in these transactions between Defendants and class members

was the obligation that Defendants would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

162. Additionally, Defendants implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and class members from unauthorized disclosure or access.

163. Plaintiff and class members entered into implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiff and class members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

164. Plaintiff and class members would not have provided and entrusted their PII to Defendants or would have paid less for Defendants' services in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the PII of Plaintiff and class members was critical to realizing the intent of the parties.

165. The nature of Defendants' implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and class members' PII in order to prevent harm and prevent present and continuing increased risk.

166. Defendants breached their implied contract with Plaintiff and class members by failing to reasonably safeguard and protect Plaintiff's and class members' PII, which was compromised as a result of the Data Breach.

167. As a direct and proximate result of Defendants' breaches, Plaintiff and class members sustained actual losses and damages as described in detail above, including that they did not receive the benefits of the bargains for which they paid, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

168. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

169. Forefront Dermatology occupied a position of advisor or counselor to its patients and employees such that Forefront Dermatology would reasonably inspire confidence that it would act in good faith and in the best interest of its patients and employees. Accordingly, a fiduciary relationship exists between Forefront Dermatology and its patients and/or employees, including Plaintiff and class members.

170. By failing to implement and maintain reasonable safeguards to protect their PII, failing to comply with industry-standard data security practices, failing to disclose critical information regarding the nature and extent of the Data Breach, and allowing a third-party hacker to release their PII on the dark web, Forefront Dermatology intentionally or negligently failed to act in good faith and solely for the benefit of Plaintiff and class members.

171. Forefront Dermatology's failure to act solely for the benefit of Plaintiff and class members was a real and meaningful factor in bringing about their injuries.

172. As a direct and proximate result of Forefront Dermatology's breach of fiduciary duty, Plaintiff and class members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT VI
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

173. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

174. Forefront Dermatology required Plaintiff and class members to provide their PII as a condition of treatment and/or for purposes of employment. Such information was highly personal, sensitive, and not generally known.

175. Forefront Dermatology expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

176. Forefront Dermatology disclosed the PII to unauthorized third parties by failing to implement and maintain reasonable safeguards to protect its patients' and employees' PII and failing to comply with industry-standard data security practices.

177. As a direct and proximate result of Forefront Dermatology's breach of confidence, Plaintiff and class members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT VII
BAILMENT
(On Behalf of Plaintiff and the Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

178. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

179. Plaintiff and class members delivered and entrusted their PII to Forefront Dermatology for the purpose of receiving medical services or employment.

180. In delivering their PII to Forefront Dermatology, Plaintiff and class members intended and understood that to Forefront Dermatology would adequately safeguard it.

181. Forefront Dermatology accepted possession of Plaintiff's and class members' PII and, in doing so, understood that Plaintiff and class members expected Forefront Dermatology to reasonably and adequately safeguard such information. Accordingly, a constructive bailment was established for the mutual benefit of the parties.

182. During the bailment, Forefront Dermatology owed a duty to Plaintiff and class members to exercise reasonable care, diligence, and prudence in protecting their PII.

183. Forefront Dermatology breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and class members' PII, resulting in the unlawful and unauthorized access to and misuse of such information.

184. As a direct and proximate result of Forefront Dermatology's breach, Plaintiff and class members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT VIII
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Patient Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

185. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

186. Plaintiff and class members had a reasonable expectation of privacy in the highly sensitive PII they provided to Forefront Dermatology in order to receive medical care.

187. Forefront disclosed Plaintiff's PII, including highly sensitive medical records, diagnoses, and treatment information, to a known ransomware group without consent in a manner that would be highly offensive to a reasonable person.

188. Forefront acted intentionally or with reckless disregard as it knew it had not adequately invested in data security or implemented reasonable data security measures to protect against the theft of PII.

189. As a direct and proximate result of Forefront Dermatology's invasion of privacy, Plaintiff and class members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiff and class members seek an award of nominal damages.

COUNT IX
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Patient Class, or, alternatively, Plaintiff and the Illinois Subclass, against the Defendants)

190. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein and assert this claim in the alternative to their breach of contract claims to the extent necessary.

191. Plaintiff and class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by the Defendants and which was ultimately stolen in the Data Breach. This information has independent value.

192. Plaintiff and class members conferred a monetary benefit on Defendants in the form of payments for medical services, including those paid indirectly by Plaintiff to the Defendants responsible for providing medical care.

193. Defendants appreciated and had knowledge of the benefits conferred upon them by Plaintiff and class members.

194. The price for medical and healthcare services that Plaintiff and class members paid (directly or indirectly) to Defendants should have been used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

195. Likewise, in exchange for receiving Plaintiff's and class members' valuable PII, which Defendants were able to use for their own business purposes and which provided actual value to Defendants, Defendants were obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

196. As a result of Defendants' conduct, Plaintiff and class members suffered actual

damages as described herein. Under principals of equity and good conscience, Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds they received from Plaintiff and class members, including damages equaling the (1) difference in value between medical and healthcare services that included implementation of reasonable data privacy and security practices that Plaintiff and class members paid for; and (2) the services without reasonable data privacy and security practices that they actually received.

COUNT X
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class against Defendants)

197. Plaintiff restate and re-allege the preceding paragraphs as if fully set forth herein.

198. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

199. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and class members from further cyberattacks and data breaches that could compromise their PII.

200. Defendants still possess PII pertaining to Plaintiff and class members, which means their PII remains at risk of further breaches because Defendants' data security measures remain inadequate. Plaintiff continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that additional compromises of their PII will occur in the future.

201. Pursuant to the Declaratory Judgment Act, Plaintiff seek a declaration that: (a) Defendants' existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendants must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' PII if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Forefront Dermatology's systems on a periodic basis, and ordering Forefront Dermatology to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. encrypting PII and segmenting PII by, among other things, creating firewalls and access controls so that if one area of Forefront Dermatology's systems is compromised, hackers cannot gain access to other portions of Forefront Dermatology's systems;

e. purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions;

f. conducting regular database scanning and security checks;

g. conducting regular employee education regarding best security practices;

h. implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

Plaintiff, on behalf of herself and all class members, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a jury trial on all claims so triable.

Date: September 20, 2021

Respectfully submitted,

/s/ *K. Scott Wagner*
K. Scott Wagner (Bar No. 1004668)
Shauna D. Manion (Bar No. 1091704)
MALLERY, S.C.
31 North Jackson Street, Suite 900
Milwaukee Wisconsin 53202
Telephone: (414) 727-6270
swagner@mallerysc.com

Jason S. Hartley*
Jason M. Lindner*
Fatima G. Brizuela*
HARTLEY LLP
101 W. Broadway, Suite 820
San Diego, CA 92101
Telephone: (619) 400-5822
hartley@hartleyllp.com
lindner@hartleyllp.com
brizuela@hartleyllp.com
*Pro Hac Vice forthcoming

Vincent J. Esades*
HEINS MILLS & OLSON, P.L.C.
310 Clifton Avenue
Minneapolis, MN 55403
(612) 338-4605
vesades@heinsmills.com
*Pro Hac Vice forthcoming

Attorneys for Plaintiff and the Class